# VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI

*ai sensi del GDPR 2016/679 e normativa nazionale in vigore*

| | |
|---|---|
| Azienda/Organizzazione | **ISTITUTO COMPRENSIVO STATALE FALCOMATA' - ARCHI** |

| | |
|---|---|
| **TITOLARE** | CORRADO SERAFINA |

| | |
|---|---|
| **SEDE** | Sede<br>ISTITUTO COMPRENSIVO STATALE FALCOMATA' – ARCHI<br>Via Montello 7,<br>89122 - Reggio Calabria |

Data revisione: 01/09/2022

# VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI

La DPIA, acronimo di Data Protection Impact Assessment, è una valutazione preliminare, eseguita dal titolare del trattamento dei dati personali, relativa agli impatti a cui andrebbe incontro un trattamento laddove dovessero essere violate le misure di protezione dei dati.

In linea con l'approccio basato sul rischio adottato dal regolamento generale sulla protezione dei dati, non è obbligatorio svolgere una valutazione d'impatto sulla protezione dei dati per ciascun trattamento; è necessario realizzare una valutazione d'impatto sulla protezione dei dati soltanto quando la tipologia di trattamento "può presentare un rischio elevato per i diritti e le libertà delle persone fisiche" (articolo 35 del Regolamento 2016/679).

## OBBLIGO DPIA

Ai sensi dell'articolo 35, paragrafo 3 del Regolamento 2016/679 la valutazione è stata effettuata nei casi in cui un trattamento può presentare rischi elevati, ossia quando:

a. una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;
b. il trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10;
c. la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

## CRITERI DA CONSIDERARE PER OBBLIGO DPIA

Nel percorso di analisi sono stati presi in considerazione i seguenti 9 criteri:

1. Valutazione o assegnazione di un punteggio
2. Processo decisionale automatizzato che ha effetto giuridico o incide in modo analogo significativamente
3. Monitoraggio sistematico
4. Dati sensibili o aventi carattere altamente personale
5. Trattamento di dati su larga scala
6. Creazione di corrispondenze o combinazione di insieme di dati
7. Dati relativi ad interessati vulnerabili
8. Uso innovativo o applicazione di nuove soluzioni tecnologiche
9. Trattamento che impedisce agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto

Nel caso in cui un'attività di trattamento dati soddisfa due o più criteri viene eseguita la valutazione d'impatto sulla protezione dei dati.

## REVISIONE

Secondo le buone prassi, la valutazione d'impatto sulla protezione dei dati viene riesaminata continuamente e rivalutata con regolarità.

# ALGORITMO VALUTAZIONE

## 1° STEP: identificazione dei trattamenti

Il primo step consiste nel censire tutte le attività di trattamento di dati personali specificandone:

- dati identificativi (Sede, struttura, funzioni),
- finalità,
- tipologia di dati personali trattati,
- categorie di interessati,
- destinatari,
- modalità di elaborazione dati (cartacea, elettronica, mista),
- termine cancellazione dati,
- eventuale trasferimento paesi terzi,
- misure di sicurezza.

## 2° STEP: valutazione del rischio e individuazione criteri per DPIA

Un rischio è uno scenario che descrive un evento e le sue conseguenze, stimato in termini di gravità e probabilità. L'entità dei rischi viene ricavata assegnando un opportuno valore alla **probabilità di accadimento (P)** ed alle **conseguenze** di tale evento **(C)**. Dalla combinazione di tali grandezze si ricava la matrice di rischio la cui entità è data dalla relazione:

**LR = P X C**

**LR = livello di rischio**
**P = probabilità di accadimento**
**C = conseguenze**

Alla **probabilità di accadimento dell'evento P** è associato un indice numerico rappresentato nella seguente tabella:

| PROBABILITA' DELL'EVENTO | |
|---|---|
| 1 | Improbabile |
| 2 | Poco probabile |
| 3 | Probabile |
| 4 | M. Probabile |
| 5 | Quasi certo |

Alle **conseguenze** (C) è associato un indice numerico rappresentato nella seguente tabella:

| CONSEGUENZE | |
|---|---|
| 1 | Trascurabili |
| 2 | Marginali |
| 3 | Limitate |
| 4 | Gravi |
| 5 | Gravissime |

## MATRICE DEI RISCHI

La matrice che scaturisce dalla combinazione di **probabilità** e **conseguenze** è rappresentata in figura seguente:

| Probabilità | | | | | | |
|---|---|---|---|---|---|---|
| | 5 | 5 | 10 | 15 | 20 | 25 |
| | 4 | 4 | 8 | 12 | 16 | 20 |
| | 3 | 3 | 6 | 9 | 12 | 15 |
| | 2 | 2 | 4 | 6 | 8 | 10 |
| | 1 | 1 | 2 | 3 | 4 | 5 |
| | | 1 | 2 | 3 | 4 | 5 |
| | | Conseguenze | | | | |

| Entità Rischio | Valori di riferimento |
|---|---|
| Accettabile | *(1 ≤ **LR** ≤ 3)* |
| Medio - basso | *(4 ≤ **LR** ≤ 6)* |
| Rilevante | *(8 ≤ **LR** ≤ 12)* |
| Alto | *(15 ≤ **LR** ≤ 25)* |

Si ricava, così, per ogni attività di trattamento un Livello di Rischio (di potenziale perdita, divulgazione, modifica, distruzione non autorizzata di dati).

In questo step viene anche ricercata la presenza di criteri di obbligo DPIA:

1. Valutazione o assegnazione di un punteggio
2. Processo decisionale automatizzato che ha effetto giuridico o incide in modo analogo significativamente
3. Monitoraggio sistematico

4. Dati sensibili o aventi carattere altamente personale
5. Trattamento di dati su larga scala
6. Creazione di corrispondenze o combinazione di insieme di dati
7. Dati relativi ad interessati vulnerabili
8. Uso innovativo o applicazione di nuove soluzioni tecnologiche
9. Trattamento che impedisce agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto

Se vi è presenza di almeno due criteri e/o il Livello di Rischio risulta ALTO, l'attività richiede la DPIA.

### 3 STEP: DPIA – valutazione del rischio normalizzato

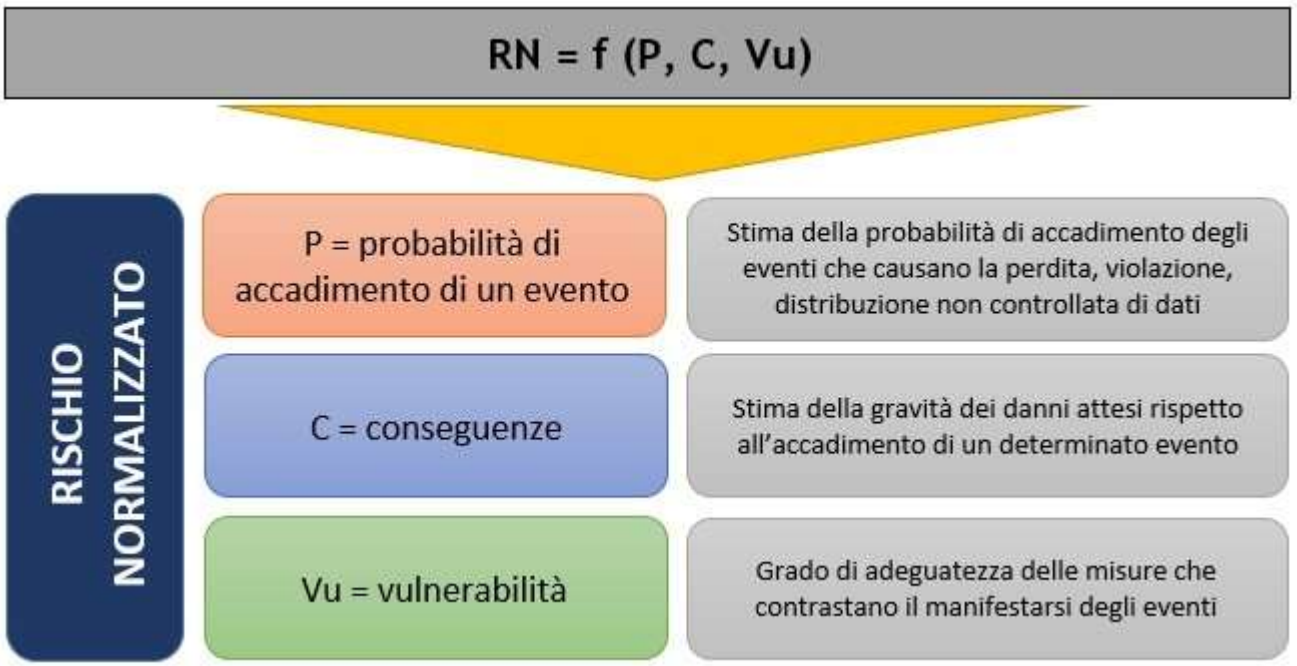
Ai sensi dell'art. 35 del GDPR, vengono individuate tutte le attività di trattamento che in prima analisi presentano un livello di rischio alto e/o prevendono due o più criteri di obbligo DPIA.
Nel caso in cui, quindi, l'indice di rischio si colloca nel range 15 ÷ 25, l'attività necessita di una valutazione di impatto mediante un'analisi approfondita di alcuni aspetti.
La DPIA si basa su un'analisi dei rischi più dettagliata cercando di dare un peso ai possibili controlli applicabili, ricavando, così, un indice di rischio "normalizzato" rispetto al contesto aziendale.

Il rischio viene calcolato in funzione dei 3 fattori seguenti:

**RN = f (P, C, Vu)**

Dove:

P = probabilità
C = conseguenze generate dall'evento




V = vulnerabilità rispetto al grado di adeguatezza delle misure

**In prima battuta viene ricavato il rischio intrinseco Ri come prodotto della probabilità P e delle conseguenze C, in base agli indici numerici assegnati ad entrambi i fattori.**

Alla **probabilità P** è associato un indice numerico rappresentato nella seguente tabella:

| Probabilità | |
|---|---|
| 1 | Improbabile |
| 2 | Poco probabile |
| 3 | Probabile |
| 4 | Quasi certo |

Alle **conseguenze** (C) è associato un indice numerico rappresentato nella seguente tabella:

| CONSEGUENZE | |
|---|---|
| 1 | Trascurabili |
| 2 | Marginali |
| 3 | Limitate |
| 4 | Gravi |

Rispetto al 1 STEP, la matrice ha un range ridotto, essendo una matrice 4 x 4:

| PROBABILITÀ | | | | | |
|---|---|---|---|---|---|
| | 4 | 4 | 8 | 12 | 16 |
| | 3 | 3 | 6 | 9 | 12 |
| | 2 | 2 | 4 | 6 | 8 |
| | 1 | 1 | 2 | 3 | 4 |
| | | 1 | 2 | 3 | 4 |
| | | CONSEGUENZE | | | |

| RISCHIO INTRINSECO | |
|---|---|
| **Ri = P x C** | **Valori di riferimento** |
| Molto basso | *(1 ≤ **Ri** ≤ 2)* |
| Basso | *(3 ≤ **Ri** ≤ 4)* |
| Rilevante | *(6 ≤ **Ri** ≤ 9)* |
| Alto | *(12 ≤ **Ri** ≤ 16)* |

Il rischio intrinseco viene ricavato prendendo in considerazione tutti i possibili Pericoli e Rischi.
Di seguito la suddivisione delle aree di pericolo con i rischi generati.

| PERICOLO | RISCHI |
|---|---|
| Agenti fisici (incendio, allagamento, attacchi esterni) | • Perdita<br>• Distruzione non autorizzata |
| Eventi naturali (terremoti, eruzioni vulcaniche, ecc.) | • Perdita<br>• Distruzione non autorizzata |
| Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.) | • Perdita<br>• Distruzione non autorizzata<br>• Modifica non autorizzata<br>• Divulgazione non autorizzata<br>• Accesso dati non autorizzato |
| Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT) | • Perdita<br>• Distruzione non autorizzata<br>• Modifica non autorizzata<br>• Divulgazione non autorizzata<br>• Accesso dati non autorizzato |
| Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.) | • Perdita<br>• Distruzione non autorizzata<br>• Modifica non autorizzata<br>• Divulgazione non autorizzata<br>• Accesso dati non autorizzato |
| Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | • Perdita<br>• Distruzione non autorizzata<br>• Modifica non autorizzata<br>• Divulgazione non autorizzata<br>• Accesso dati non autorizzato |

Per ricavare il Rischio Normalizzato RN, viene introdotto il fattore Vulnerabilità Vu che fornisce un'indicazione circa l'adeguatezza delle misure di sicurezza attuate per ogni rischio.

Alla **Vulnerabilità** (Vu) è associato un indice numerico rappresentato nella seguente tabella:

| | VULNERABILITA' | Valore |
|---|---|---|
| 1 | Adeguate | 0,25 |
| 2 | Parzialmente adeguate | 0,5 |
| 3 | Inadeguate | 1 |

Per ogni rischio vengono indicate le misure di sicurezza adottate, per ognuna delle quali viene definito il grado di adeguatezza, assegnando uno dei possibili valori:

- 0,25;
- 0,5;
- 1.

Per ricavare il valore del rischio normalizzato RN viene moltiplicato il Rischio Intrinseco Ri con il valore peggiore assegnato alle misure di sicurezza relativamente a quel rischio.

| | | | | | |
|---|---|---|---|---|---|
| Vu | 1 | 1 < ***RN*** ≤ 2 | 3 ≤ ***RN*** ≤ 4 | 6 ≤ ***RN*** ≤ 9 | 12 ≤ ***RN*** ≤ 16 |
| | 0,5 | 0,5 < ***RN*** ≤ *1* | 1,5 ≤ ***RN*** ≤ 2 | 3 < ***RN*** ≤ 5 | 6 ≤ ***RN*** ≤ 8 |
| | 0,25 | 0,25 ≤ ***RN*** ≤ 0,5 | 0,75 ≤ ***RN*** ≤ 1 | 1,5 ≤ ***RN*** < 3 | 3 ≤ ***RN*** ≤ 4 |
| | | 1 ≤ ***Ri*** ≤ 2 | 3 ≤ ***Ri*** ≤ 4 | 6 ≤ ***Ri*** ≤ 9 | 12 ≤ ***Ri*** ≤ 16 |
| | | Ri | | | |

| RISCHIO NORMALIZZATO | |
|---|---|
| **RN = Ri x Vu** | **Valori di riferimento** |
| Molto basso | 0,25 ≤ ***RN*** ≤ 1 |
| Basso | 1 < ***RN*** < 3 |
| Rilevante | 3 ≤ ***RN*** ≤ 9 |
| Alto | 12 ≤ ***RN*** ≤ 16 |

Se, a valle dell'analisi DPIA, l'attività ricade comunque in fascia **ALTA**, il Titolare attiva l'iter di consultazione del Garante.

## RISULTATI DPIA

Di seguito, viene riportata l'analisi di tutte le attività di trattamento per cui si è resa necessaria la valutazione di impatto sulla protezione dei dati.

## Elenco attività sottoposte a DPIA

- Attività didattiche

| Struttura | SEDE LEGALE ED OPERATIVA |
|---|---|

| Personale coinvolto | |
|---|---|
| **Titolare del trattamento** | CORRADO SERAFINA (DIRIGENTE) |
| **Persone autorizzate** | C CORRADO SERAFINA (DIRIGENTE)<br>NERI VALERIA (DSGA)<br>BOMBARDIERE PASQUALE (ASS.AMM.)<br>CUTRUPI FRANCESCA, (ASS.AMM.)<br>MALARA GIUSEPPE (ASS.AMM.)<br>MARRA ERNESTA (ASS.AMM.)<br>NAPOLI ADRIANA (ASS.AMM.)<br>SPINELLA ANGELA CARMELA (ASS.AMM.)<br>ZIRILLI CARMELA STEFANIA (ASS.AMM.)<br>TOSCANO CARMEN (1° COLLABORATORE DS)<br>ARCONTE MARIA FILIPPA (2° COLLABORATORE DS)<br>ALBANO ROSARIA CARMELA (COORD. DID. PLESSO)<br>CAPPELLACCIO PATRIZIA (COORD. DID. PLESSO)<br>CALARCO MILENA (COORD. DID. PLESSO)<br>LA FACE FRANCESCA (COORD. DID. PLESSO)<br>MARRA ANTONIETTA ROSA (COORD. DID. PLESSO)<br>MUSOLINO ROSSANA (COORD. DID. PLESSO)<br>PANSERA MARIA (COORD. DID. PLESSO)<br>SORGONA' GEMMA LUCIA (COORD. DID. PLESSO)<br>CARIDI BARBARA (REFERENTE REGISTRO ELETTRONICO)<br>COTRONEO CATERINA GIOVANNA (ANIMATORE DIGITALE)<br>DI STEFANO ERNESTA TERESA (FUNZIONE STRUMENTALE)<br>LO SCHIAVO RITA (FUNZIONE STRUMENTALE)<br>MALASPINA MAURIZIO (FUNZIONE STRUMENTALE)<br>QUATTRONE GIOVANNI (FUNZIONE STRUMENTALE)<br>ZANGARI FRANCESCA (FUNZIONE STRUMENTALE)<br>SETTIMIO SAVERIO MARIA (AMMINISTRATORE DI SISTEMA) |

| | |
|---|---|
| **Partners - Responsabili esterni** | MUSOLINO GIUSEPPE, (Medico Competente) |
| **Altro** | Personale con diritto di accesso:<br><br>DOCENTI CON NOMINA DI INCARICO DI CUI SI ALLEGA ELENCO AL REGISTRO |

| **Processo di trattamento** | |
|---|---|
| **Descrizione** | Attività didattiche |
| **Fonte dei dati personali** | Forniti da terzi<br>Raccolti direttamente |
| **Base giuridica per il trattamento per dati comuni (art. 6 GDPR)** | Consenso<br>Contratto |
| **Base giuridica per il trattamento per dati particolari (art. 9 GDPR)** | Consenso<br>Contratto<br>Legge |
| **Finalità del trattamento** | Adempimento di obblighi fiscali o contabili;<br>Attività di consulenza;<br>Contratto di assunzione;<br>Gestione dei fornitori (contratti, ordini, arrivi, fatture);<br>Gestione del personale;<br>Gestione dell'utenza<br>Igiene e sicurezza del lavoro;<br>Informazione per via telematica;<br>Newsletter;<br>Relazioni con il pubblico;<br>Pubblicità e promozione iniziative e di soggetti terzi (partner);<br>Analisi del bisogno e progettazione servizi;<br>Erogazione servizi e attività formative, sociali, ricreative, educative, socio-assistenziali;<br>Progettazione educativa;<br>Raccolta fondi;<br>Iscrizione e aggiornamento dei dati utenti in software gestionale SIDI MIUR<br><br>Adempimento di obblighi fiscali o contabili;<br>Attività di consulenza;<br>Contratto di assunzione; |
| **Tipo di dati personali** | Dati personali:<br><br>Codice fiscale ed altri numeri di identificazione personale (carte sanitarie);<br>Curriculum di studi e accademico, pubblicazioni, articoli, monografie, relazioni, materiale audiovisivo, titoli di studio, ecc.<br>Dati identificativi (ragione o denominazione sociale, ovvero nome e cognome delle persone fisiche, indirizzo sede, telefono, fax, e-mail, dati fiscali, ecc.);<br>Dati relativi alla famiglia e a situazioni personali; |

| | |
|---|---|
| | Dati relativi alla famiglia e a situazioni personali (stato civile, minori, figli, soggetti a carico, consanguinei, altri appartenenti al nucleo familiare);<br>Dati relativi all'attività economica e commerciale;<br>Lavoro (occupazione attuale e precedente, informazioni sul reclutamento, sul tirocinio o sulla formazione professionale, informazioni sulla sospensione o interruzione del rapporto di lavoro o sul passaggio ad altra occupazione, curriculum vitae;<br>Nominativo, indirizzo o altri elementi di identificazione personale (nome, cognome, età, sesso, luogo e data di nascita, indirizzo privato, indirizzo di lavoro).<br><br>Dati particolari:<br>Sensibili (medici) e giudiziari (situazione individuale e familiare) |
| **Categorie di interessati** | Aderenti ad associazioni politiche, religiose o sindacali;<br>Agenti e Rappresentanti;<br>Artigiani;<br>Clienti ed utenti;<br>Collaboratori;<br>Commercianti;<br>Condomini;<br>Consulenti e liberi professionisti, anche in forma associata;<br>Dipendenti;<br>Enti;<br>Istituti di credito e assicurativi<br>Familiari dell'interessato;<br>Fornitori;<br>Imprenditori e piccoli imprenditori;<br>Industrie;<br>Lavoratori Autonomi;<br>Personale pubblico dirigenziale e magistrati;<br>PMI (Piccole e Medie Imprese);<br>Potenziali clienti;<br>Soci associati ed iscritti;<br>Soggetti o organismi pubblici. |
| **Categorie di destinatari** | ASL e Commissioni mediche<br>Altre amministrazioni pubbliche;<br>Autorità di vigilanza e controllo;<br>Camere di commercio, industria, artigianato ed agricoltura;<br>Clienti ed utenti;<br>Consulenti e liberi professionisti anche in forma associata;<br>Datore di lavoro;<br>Enti locali;<br>Istituti di credito e assicurativi<br>Forze di polizia;<br>Persone autorizzate;<br>Enti previdenziali ed assistenziali;<br>Interessati;<br>Medico competente;<br>Ordini e collegi professionali;<br>Organizzazioni sindacali e patronati;<br>Organismi paritetici in materia di lavoro;<br>Rappresentante dei lavoratori per la sicurezza;<br>Enti pubblici e privati in relazione ai rapporti di lavoro e di consulenza;<br>Compagnie di assicurazione con cui l'Istituto abbia stipulato eventuali polizze;<br>Agenzie di viaggio e/o strutture alberghiere e/o enti gestori degli accessi a musei, gallerie, monumenti, fiere, in occasione di visite |

| | |
|---|---|
| | guidate e viaggi di istruzione;<br>Compagnie teatrali, compagnie circensi in occasioni di spettacoli e/o attività integrative che coinvolgano gli allievi e/o il personale della scuola;<br>Scuole, enti e/o associazioni accreditati per la gestione di corsi di aggiornamento e formazione;<br>Enti certificatori di competenze linguistiche o informatiche;<br>Imprese, ditte o studi professionali in occasioni di stage o esperienze di alternanza scuola-lavoro |
| **Informativa** | Si |
| **Profilazione** | SI: Bisogni del cliente, caratteristiche personali, emotive ed educative. Abitudini e dinamiche familiari, del singolo e del minore. |
| **Dati particolari** | SI: Sensibili e giudiziari.<br>- Acquisizione in alcuni casi di dati medici, diagnosi, patologie, terapie.<br>- Acquisizione dati giudiziari se necessari, riferiti alla situazione familiare del minore. (esempio provvedimenti di affidamento, separazione,….)<br>- Acquisizione dati religiosi delle famiglie<br>- Acquisizione dati sindacali dei dipendenti |
| **Consenso minori** | SI |
| **Frequenza trattamento** | Giornaliera |
| **Termine cancellazione dati** | I dati saranno trattati per tutto il tempo necessario allo svolgimento del rapporto commerciale in essere e per i successivi dieci anni dalla data di acquisizione degli stessi. |
| **Trasferimento dati (paesi terzi)** | SI: dati dell'alunno per trasferimento in altra scuola estero e/o per stage alunni in altro paese) |
| **Autorizzazione del Garante** | Non presente |

| **Modalità di elaborazione dati: Mista - elettronica e cartacea** | |
|---|---|
| **Strumenti** | Software gestionale<br>Pacchetto Office<br>Faldoni e Cartelle cartacee ed informatiche |
| **Archiviazione** | Stanza archivio con diniego di accesso al pubblico<br>Armadio chiuso a chiave |
| **Strutture informatiche di archiviazione** | |
| **Strutture informatiche di backup** | |
| **Archivio Informatico Scuola** | Struttura interna : Server con Nas – Hard Disk Esterni |
| **Sede di riferimento** | ISTITUTO COMPRENSIVO STATALE FALCOMATA' – ARCHI<br>Sede Via Montello 7, 89122 - Reggio Calabria |
| **Frequenza di backup** | 1 giorni |
| **Tempo di storicizzazione** | 30 giorni |
| **Personale con diritti di accesso** | CORRADO SERAFINA, (DIRIGENTE) |

| | |
|---|---|
| | CORRADO SERAFINA (DIRIGENTE)<br>NERI VALERIA (DSGA)<br>BOMBARDIERE PASQUALE (ASS.AMM.)<br>CUTRUPI FRANCESCA, (ASS.AMM.)<br>MALARA GIUSEPPE (ASS.AMM.)<br>MARRA ERNESTA (ASS.AMM.)<br>NAPOLI ADRIANA (ASS.AMM.)<br>SPINELLA ANGELA CARMELA (ASS.AMM.)<br>ZIRILLI CARMELA STEFANIA (ASS.AMM.)<br>TOSCANO CARMEN (1° COLLABORATORE DS)<br>ARCONTE MARIA FILIPPA (2° COLLABORATORE DS)<br>ALBANO ROSARIA CARMELA (COORD. DID. PLESSO)<br>CAPPELLACCIO PATRIZIA (COORD. DID. PLESSO)<br>CALARCO MILENA (COORD. DID. PLESSO)<br>LA FACE FRANCESCA (COORD. DID. PLESSO)<br>MARRA ANTONIETTA ROSA (COORD. DID. PLESSO)<br>MUSOLINO ROSSANA (COORD. DID. PLESSO)<br>PANSERA MARIA (COORD. DID. PLESSO)<br>SORGONA' GEMMA LUCIA (COORD. DID. PLESSO)<br>CARIDI BARBARA (REFERENTE REGISTRO ELETTRONICO)<br>COTRONEO CATERINA GIOVANNA (ANIMATORE DIGITALE)<br>DI STEFANO ERNESTA TERESA (FUNZIONE STRUMENTALE)<br>LO SCHIAVO RITA (FUNZIONE STRUMENTALE)<br>MALASPINA MAURIZIO (FUNZIONE STRUMENTALE)<br>QUATTRONE GIOVANNI (FUNZIONE STRUMENTALE)<br>ZANGARI FRANCESCA (FUNZIONE STRUMENTALE)<br>SETTIMIO SAVERIO MARIA (AMMINISTRATORE DI SISTEMA)<br><br>MUSOLINO GIUSEPPE, (Medico Competente) |
| **Note** | Personale con diritto di accesso:<br><br>DOCENTI CON NOMINA DI INCARICO DI CUI SI ALLEGA ELENCO AL REGISTRO |

| | |
|---|---|
| **Software utilizzati** | SOFTWARE GESTIONALE – FILE EXCEL<br>SERVER CLOUD CERTIFICATI UTILIZZATI: Axios Cloud – Sidi Miur |

| **VALUTAZIONE DEL LIVELLO DI RISCHIO** | | | |
|---|---|---|---|
| **RISCHIO** | **PROBABILITÀ** | **CONSEGUENZE** | **LIVELLO DI RISCHIO** |
| Accesso dati non autorizzato | Poco probabile | Gravissime | Rilevante |
| Distruzione non autorizzata | Poco probabile | Gravi | Rilevante |
| Divulgazione non autorizzata | Poco probabile | Gravissime | Rilevante |
| Modifica non autorizzata | Poco probabile | Gravissime | Rilevante |
| Perdita | Probabile | Gravi | Rilevante |

**MISURE DI SICUREZZA TECNICHE ED ORGANIZZATIVE**

- Autorizzazione del singolo incaricato al trattamento e alla modifica dei dati
- Dispositivi antincendio
- E' applicata una gestione della password degli utenti
- E' applicata una procedura per la gestione degli accessi
- E' eseguita la DPIA
- E' presenta una politica per la sicurezza e la protezione dei dati
- Esistono procedure e disposizioni scritte per l'individuazione delle modalità con le quali il titolare può assicurare la disponibilità dei dati
- Esistono procedure per l'individuazione del custode delle password
- I sistemi di autorizzazione prevedono: la presenza di diversi profili di autorizzazione, l'individuazione preventiva per incaricato, l'individuazione preventiva per classi omogenee di incaricati, la verifica almeno annuale dei profili
- Impianto elettrico dotato di misure salvavita atte anche ad evitare cortocircuiti e possibili incendi
- Le password sono costituite da almeno otto caratteri alfanumerici
- Le password sono modificate al primo utilizzo
- Le password sono modificate ogni 3 mesi
- Le procedure sono riesaminate con cadenza predefinita
- L'impianto elettrico è certificato ed a norma
- Porte dotate di serratura in tutti i locali contenenti fisicamente le banche dati elettroniche e cartacee
- Registrazione e deregistrazione degli utenti
- Sistemi di allarme e di sorveglianza anti-intrusione
- Sono applicate regole per la gestione delle password.
- Sono definiti i ruoli e le responsabilità
- Sono definiti i termini di conservazione e le condizioni di impiego dei dati.
- Sono gestiti i back up
- Sono stabiliti programmi di formazione e sensibilizzazione
- Sono utilizzati software antivirus e anti intrusione
- Viene eseguita opportuna manutenzione
- Viene eseguita una regolare formazione del personale

## VALUTAZIONE ADEGUATEZZA DELLE MISURE DI SICUREZZA ADOTTATE

| MISURE DI SIUREZZA | PERICOLI ASSOCIATI | LIVELLO DI ADEGUATEZZA |
|---|---|---|
| Autorizzazione del singolo incaricato al trattamento e alla modifica dei dati | Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | Adeguate |
| Dispositivi antincendio | Agenti fisici (incendio, allagamento, attacchi esterni) | Parzialmente adeguate |
| E' applicata una gestione della password degli utenti | • Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)<br>• Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)<br>• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | Adeguate |
| E' applicata una procedura per la gestione degli accessi | • Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)<br>• Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.)<br>• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | Adeguate |
| E' eseguita la DPIA | • Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)<br>• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | Parzialmente adeguate |
| E' presenta una politica per la sicurezza e la protezione dei dati | • Eventi naturali (terremoti, eruzioni vulcaniche, ecc.)<br>• Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)<br>• Azioni non autorizzate (Errori | Adeguate |

| | | |
|---|---|---|
| | volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | |
| Esistono procedure e disposizioni scritte per l'individuazione delle modalità con le quali il titolare può assicurare la disponibilità dei dati | • Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT) | Parzialmente adeguate |
| Esistono procedure per l'individuazione del custode delle password | • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | Adeguate |
| I sistemi di autorizzazione prevedono: la presenza di diversi profili di autorizzazione, l'individuazione preventiva per incaricato, l'individuazione preventiva per classi omogenee di incaricati, la verifica almeno annuale dei profili | Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | Adeguate |
| Impianto elettrico dotato di misure salvavita atte anche ad evitare cortocircuiti e possibili incendi | • Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.)<br>• Agenti fisici (incendio, allagamento, attacchi esterni) | Adeguate |
| Le password sono costituite da almeno otto caratteri alfanumerici | • Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)<br>• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | Adeguate |
| Le password sono modificate al primo utilizzo | • Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)<br>• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | Adeguate |
| Le password sono modificate ogni 3 mesi | • Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)<br>• Azioni non autorizzate (Errori | Parzialmente adeguate |

| | | |
|---|---|---|
| | volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | |
| Le procedure sono riesaminate con cadenza predefinita | • Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)<br>• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | Adeguate |
| L'impianto elettrico è certificato ed a norma | • Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.)<br>• Agenti fisici (incendio, allagamento, attacchi esterni) | Adeguate |
| Porte dotate di serratura in tutti i locali contenenti fisicamente le banche dati elettroniche e cartacee | • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | Adeguate |
| Registrazione e deregistrazione degli utenti | • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)<br>• Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.) | Adeguate |
| Sistemi di allarme e di sorveglianza anti-intrusione | • Agenti fisici (incendio, allagamento, attacchi esterni)<br>• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)<br>• Eventi naturali (terremoti, eruzioni vulcaniche, ecc.) | Adeguate |
| Sono applicate regole per la gestione delle password. | • Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)<br>• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | Adeguate |
| Sono definiti i ruoli e le responsabilità | • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | Adeguate |
| Sono definiti i termini di conservazione e le condizioni di impiego dei dati. | • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | Adeguate |

| | | |
|---|---|---|
| | • Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.) | |
| Sono gestiti i back up | • Eventi naturali (terremoti, eruzioni vulcaniche, ecc.)<br>• Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)<br>• Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.)<br>• Agenti fisici (incendio, allagamento, attacchi esterni) | Adeguate |
| Sono stabiliti programmi di formazione e sensibilizzazione | Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | Parzialmente adeguate |
| Sono utilizzati software antivirus e anti intrusione | • Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)<br>• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | Adeguate |
| Viene eseguita opportuna manutenzione | • Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT) | Adeguate |
| Viene eseguita una regolare formazione del personale | • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | Parzialmente adeguate |

## VALUTAZIONE DEI RISCHI

| PERICOLO | | |
|---|---|---|
| Agenti fisici (incendio, allagamento, attacchi esterni) | | |
| **RISCHI** | | |
| • Perdita<br>• Distruzione non autorizzata | | |
| **VALUTAZIONE RISCHIO INTRINSECO** | | |
| **Probabilità** | **Conseguenza** | **Rischio intrinseco - Ri** |
| Poco probabile | Gravi | Rilevante |
| **VALUTAZIONE RISCHIO NORMALIZZATO**<br>*Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi* | | |
| **Rischio intrinseco - Ri** | **Vulnerabilità - Vu** | **Rischio normalizzato - RN** |
| Rilevante | 0,5 | Rilevante |

| PERICOLO | | |
|---|---|---|
| Eventi naturali (terremoti, eruzioni vulcaniche, ecc.) | | |
| **RISCHI** | | |
| • Perdita<br>• Distruzione non autorizzata | | |
| **VALUTAZIONE RISCHIO INTRINSECO** | | |
| **Probabilità** | **Conseguenza** | **Rischio intrinseco - Ri** |
| Poco probabile | Gravi | Rilevante |
| **VALUTAZIONE RISCHIO NORMALIZZATO**<br>*Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi* | | |
| **Rischio intrinseco - Ri** | **Vulnerabilità - Vu** | **Rischio normalizzato - RN** |
| Rilevante | 0,25 | Basso |

| PERICOLO | | |
|---|---|---|
| Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.) | | |
| **RISCHI** | | |
| • Perdita<br>• Distruzione non autorizzata<br>• Modifica non autorizzata<br>• Divulgazione non autorizzata<br>• Accesso dati non autorizzato | | |
| **VALUTAZIONE RISCHIO INTRINSECO** | | |
| **Probabilità** | **Conseguenza** | **Rischio intrinseco - Ri** |
| Poco probabile | Gravi | Rilevante |
| **VALUTAZIONE RISCHIO NORMALIZZATO**<br>*Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi* | | |
| **Rischio intrinseco - Ri** | **Vulnerabilità - Vu** | **Rischio normalizzato - RN** |
| Rilevante | 0,25 | Basso |

| PERICOLO | | |
|---|---|---|
| Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT) | | |
| **RISCHI** | | |
| • Perdita<br>• Distruzione non autorizzata<br>• Modifica non autorizzata<br>• Divulgazione non autorizzata<br>• Accesso dati non autorizzato | | |
| **VALUTAZIONE RISCHIO INTRINSECO** | | |
| **Probabilità** | **Conseguenza** | **Rischio intrinseco - Ri** |
| Poco probabile | Gravi | Rilevante |
| **VALUTAZIONE RISCHIO NORMALIZZATO**<br>*Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi* | | |
| **Rischio intrinseco - Ri** | **Vulnerabilità - Vu** | **Rischio normalizzato - RN** |
| Rilevante | 0,5 | Rilevante |

| PERICOLO | | |
|---|---|---|
| Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.) | | |
| **RISCHI** | | |
| • Perdita<br>• Distruzione non autorizzata<br>• Modifica non autorizzata<br>• Divulgazione non autorizzata<br>• Accesso dati non autorizzato | | |
| **VALUTAZIONE RISCHIO INTRINSECO** | | |
| **Probabilità** | **Conseguenza** | **Rischio intrinseco - Ri** |
| Poco probabile | Gravi | Rilevante |
| **VALUTAZIONE RISCHIO NORMALIZZATO**<br>*Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi* | | |
| **Rischio intrinseco - Ri** | **Vulnerabilità - Vu** | **Rischio normalizzato - RN** |
| Rilevante | 0,5 | Rilevante |

| PERICOLO | | |
|---|---|---|
| Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) | | |
| **RISCHI** | | |
| • Perdita<br>• Distruzione non autorizzata<br>• Modifica non autorizzata | | |
| **VALUTAZIONE RISCHIO INTRINSECO** | | |
| **Probabilità** | **Conseguenza** | **Rischio intrinseco - Ri** |
| Poco probabile | Gravi | Rilevante |
| **VALUTAZIONE RISCHIO NORMALIZZATO**<br>*Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi* | | |
| **Rischio intrinseco - Ri** | **Vulnerabilità - Vu** | **Rischio normalizzato - RN** |
| Rilevante | 0,5 | Rilevante |

A valle della DPIA l'attività risulta a rischio **Rilevante**